

CLAIMS

1 1. A method for privacy management, comprising:
2 providing a linked collection of interactive
3 resources through which a user is able to exchange
4 information with an enterprise that provides the
5 resources;

6 assigning respective, non-uniform privacy policies
7 to at least some of the resources regarding use of the
8 information that is exchanged through the resources;

9 providing to the user accessing a given one of the
10 resources the respective privacy policy for that
11 resource; and

12 exchanging with the user at least a portion of the
13 information that is associated with the given one of the
14 resources, subject to the provided privacy policy.

1 2. A method according to claim 1, wherein exchanging
2 the information with the user comprises receiving private
3 information submitted to the enterprise by the user.

1 3. A method according to claim 2, wherein receiving the
2 private information comprises receiving the user's
3 agreement to the privacy policy, and recording the
4 private information together with an indication of the
5 privacy policy agreed upon.

1 4. A method according to claim 2, and comprising:
2 intercepting a request from an application to use
3 the private information received from the users;
4 querying the application to determine its compliance
5 with the privacy policy subject to which the requested
6 information was received; and

7 providing the requested information subject to the
8 compliance of the application with the privacy policy.

1 5. A method according to claim 1, wherein assigning the
2 non-uniform privacy policies comprises assigning a first
3 privacy policy to a first one of the resources and a
4 second, different privacy policy to a second one of the
5 resources.

1 6. A method according to claim 5, wherein providing the
2 linked collection of interactive resources comprises
3 arranging the resources in a hierarchy of nodes that
4 comprises a root node, such that each of the nodes except
5 for the root node has a parent node in the hierarchy, and
6 wherein assigning the non-uniform privacy policies
7 comprises assigning to each of at least some of the
8 nodes, including the nodes associated with the first and
9 second resources, one or more respective privacy rules
10 regarding use of the information that is associated with
11 the node, and setting for each of the nodes a node
12 privacy policy that comprises the privacy rules assigned
13 to the node combined, for each of the nodes except the
14 root node, with the node privacy policy of its parent
15 node.

1 7. A method according to claim 5, wherein providing the
2 privacy policy to the user comprises informing the user
3 who has exchanged the information associated with the
4 first resource subject to the first privacy policy of a
5 difference in the second privacy policy relative to the
6 first privacy policy before exchanging the information
7 associated with the second resource.

1 8. A method according to claim 1, wherein assigning the
2 non-uniform privacy policies comprises assigning an

3 initial privacy policy to one of the resources, and
4 subsequently making a change in the initial privacy
5 policy so as to assign a modified privacy policy to the
6 resource, and wherein providing the privacy policy to the
7 user comprises informing a user who has exchanged
8 information with the resource subject to the initial
9 privacy policy of the change.

1 9. A method according to claim 8, wherein informing the
2 user comprises prompting the user to provide an input to
3 indicate whether the user accepts or rejects the change.

1 10. A method according to claim 1, wherein assigning the
2 privacy policies comprises storing the privacy policies
3 in a computer server belonging to the enterprise, and
4 wherein providing the privacy policy to the user
5 comprises intercepting a request by the user to access
6 the given resource and providing the privacy policy for
7 the resource responsive to the request.

1 11. A method according to claim 1, wherein the
2 collection of resources comprises a collection of Web
3 pages accessible through a Web site of the enterprise.

1 12. A method according to claim 11, wherein providing
2 the privacy policy comprises conveying the policy in a
3 standard form for presentation by a Web browser.

1 13. A method according to claim 12, wherein the standard
2 form comprises a form specified by the Platform for
3 Privacy Preferences Project (P3P).

1 14. A method according to claim 1, wherein assigning the
2 non-uniform privacy policies comprises determining a
3 rating for each of the policies based on a predetermined
4 rating scale.

1 15. A method according to claim 1, wherein assigning the
2 non-uniform privacy policies comprises defining first and
3 second user classes and defining, for a given one of the
4 resources, different first and second privacy policies,
5 respectively, for the first and second user classes, and
6 wherein providing the privacy policy to the user
7 comprises determining whether the user belongs to the
8 first or second class, and providing the first or the
9 second privacy policy accordingly.

1 16. A method for privacy management, comprising:
2 arranging a body of information in a hierarchy of
3 nodes that comprises a root node, such that each of the
4 nodes except for the root node has a parent node in the
5 hierarchy;

6 assigning to each of at least some of the nodes one
7 or more respective privacy rules regarding use of the
8 information that is associated with the node;

9 setting for each of the nodes a node privacy policy
10 that comprises the privacy rules assigned to the node
11 combined, for each of the nodes except the root node,
12 with the node privacy policy of its parent node;

13 providing to a user who accesses a given one of the
14 nodes the node privacy policy for that node; and

15 exchanging with the user at least a portion of the
16 information that is associated with the given one of the
17 nodes, subject to the provided privacy policy.

1 17. A method according to claim 16, wherein exchanging
2 the information with the user comprises receiving private
3 information submitted by the user.

1 18. A method according to claim 16, wherein arranging
2 the body of information comprises a associating the nodes
3 with respective Web pages accessible through a Web site.

1 19. A method for privacy management, comprising:

2 providing a linked collection of interactive
3 resources through which a user is able to exchange
4 information with an enterprise that provides the
5 resources, at least some of the resources having privacy
6 policies associated therewith regarding use of the
7 information that is exchanged through the resources;

8 receiving information from users who access the
9 resources subject to the privacy policies;

10 intercepting a request from an application to use
11 the information received from the users;

12 querying the application to determine its compliance
13 with the privacy policies subject to which the requested
14 information was received; and

15 providing the requested information subject to the
16 compliance of the application with the privacy policies.

1 20. A method according to claim 19, wherein the
2 collection of interactive resources comprises a
3 collection of Web pages accessible through a Web site of
4 the enterprise.

1 21. A method according to claim 19, wherein providing
2 the linked collection of resources comprises associating
3 non-uniform privacy policies with the resources, and
4 wherein receiving the information comprises receiving and
5 storing different items of the information subject to
6 different privacy rules from among the non-uniform
7 privacy policies.

1 22. A method according to claim 21, wherein providing
2 the requested information comprises checking the
3 compliance of the application with the privacy rules
4 respectively applicable to each of the items of the
5 information requested by the application.

1 23. A method according to claim 21, wherein providing
2 the requested information comprises determining that the
3 application does not comply with the rules respectively
4 applicable to a given one of the items, and refusing to
5 provide the requested information with respect to the
6 given item, while providing information regarding another
7 of the items with respect to which the application does
8 comply with the respectively applicable rules.

1 24. A method according to claim 21, wherein receiving
2 and storing the different items comprises receiving the
3 items from first and second ones of the users subject to
4 respective first and second privacy policies, and wherein
5 providing the requested information comprises checking
6 the compliance of the application with both the first and
7 the second privacy policies.

1 25. A method according to claim 19, and comprising
2 making a record of the request and of the information
3 provided responsive thereto in a log for review in a
4 subsequent privacy audit.

1 26. Apparatus for privacy management, comprising a
2 computer enterprise server arranged to provide a linked
3 collection of interactive resources through which a user
4 is able to exchange information with an enterprise that
5 provides the resources, wherein respective, non-uniform
6 privacy policies are assigned to at least some of the

7 resources regarding use of the information that is
8 exchanged through the resources, and to provide to the
9 user accessing a given one of the resources the
10 respective privacy policy for that resource and to
11 exchange with the user at least a portion of the
12 information that is associated with the given one of the
13 resources, subject to the provided privacy policy.

1 27. Apparatus according to claim 26, wherein the
2 information exchanged with the user comprises private
3 information submitted to the enterprise by the user.

1 28. Apparatus according to claim 27, wherein the server
2 is arranged to receive the user's agreement to the
3 privacy policy, and to record the private information
4 together with an indication of the privacy policy agreed
5 upon.

1 29. Apparatus according to claim 27, wherein the server
2 is further arranged to intercept a request from an
3 application to use the private information received from
4 the users, to query the application to determine its
5 compliance with the privacy policy subject to which the
6 requested information was received, and to provide the
7 requested information subject to the compliance of the
8 application with the privacy policy.

1 30. Apparatus according to claim 26, wherein the server
2 is arranged to associate a first privacy policy with a
3 first one of the resources and a second, different
4 privacy policy with a second one of the resources.

1 31. Apparatus according to claim 30, wherein the linked
2 collection of interactive resources are arranged in a
3 hierarchy of nodes that comprises a root node, such that

4 each of the nodes except for the root node has a parent
5 node in the hierarchy, and wherein the server is arranged
6 to associate with each of at least some of the nodes,
7 including the nodes associated with the first and second
8 resources, one or more respective privacy rules regarding
9 use of the information that is associated with the node,
10 and to determine for each of the nodes a node privacy
11 policy that comprises the privacy rules assigned to the
12 node combined, for each of the nodes except the root
13 node, with the node privacy policy of its parent node.

1 32. Apparatus according to claim 30, wherein the server
2 is arranged to inform the user who has exchanged the
3 information associated with the first resource subject to
4 the first privacy policy of a difference in the second
5 privacy policy relative to the first privacy policy
6 before exchanging the information associated with the
7 second resource.

1 33. Apparatus according to claim 26, wherein the server
2 is arranged to associate an initial privacy policy with
3 one of the resources, and subsequently to receive an
4 indication of a change in the initial privacy policy so
5 as to associate a modified privacy policy to the
6 resource, and to inform a user who has exchanged
7 information with the resource subject to the initial
8 privacy policy of the change.

1 34. Apparatus according to claim 33, wherein the server
2 is arranged to generate a prompt to the user to provide
3 an input to indicate whether the user accepts or rejects
4 the change.

1 35. Apparatus according to claim 26, wherein the
2 collection of resources comprises a collection of Web
3 pages accessible through a Web site of the enterprise.

1 36. Apparatus according to claim 35, wherein the server
2 is adapted to convey the policy to a client computer in a
3 standard form for presentation by a Web browser.

1 37. Apparatus according to claim 35, wherein the
2 standard form comprises a form specified by the Platform
3 for Privacy Preferences Project (P3P).

1 38. Apparatus according to claim 26, wherein the server
2 is arranged to determine a rating for each of the
3 policies based on a predetermined rating scale.

1 39. Apparatus according to claim 26, wherein the server
2 is arranged to receive a definition of first and second
3 user classes and, for a given one of the resources,
4 different first and second privacy policies,
5 respectively, for the first and second user classes, and
6 to determine whether the user belongs to the first or
7 second class and to provide the first or the second
8 privacy policy to the user accordingly.

1 40. Apparatus for privacy management, comprising a
2 computer server arranged to receive and store a body of
3 information in a hierarchy of nodes that comprises a root
4 node, such that each of the nodes except for the root
5 node has a parent node in the hierarchy, together with an
6 assignment to each of at least some of the nodes of one
7 or more respective privacy rules regarding use of the
8 information that is associated with the node, and to
9 determine for each of the nodes a node privacy policy
10 that comprises the privacy rules assigned to the node

11 combined, for each of the nodes except the root node,
12 with the node privacy policy of its parent node so as to
13 provide to a user who accesses a given one of the nodes
14 the node privacy policy for that node, and to exchange
15 with the user at least a portion of the information that
16 is associated with the given one of the nodes, subject to
17 the provided privacy policy.

1 41. Apparatus according to claim 40, wherein the
2 information exchanged with the user comprises private
3 information submitted to the server by the user.

1 42. Apparatus according to claim 40, wherein the body of
2 information comprises a collection of Web pages
3 accessible through a Web site, and wherein the server is
4 arranged to associate the nodes with respective ones of
5 the Web pages.

1 43. Apparatus for privacy management, comprising a
2 computer enterprise server arranged to provide a linked
3 collection of interactive resources through which a user
4 is able to exchange information with an enterprise that
5 provides the resources, at least some of the resources
6 having privacy policies associated therewith regarding
7 use of the information that is exchanged through the
8 resources, and to receive information from users who
9 access the resources subject to the privacy policies, and
10 to intercept a request from an application to use the
11 information received from the users, to query the
12 application to determine its compliance with the privacy
13 policies subject to which the requested information was
14 received, and to provide the requested information
15 subject to the compliance of the application with the
16 privacy policies.

1 44. Apparatus according to claim 43, wherein the
2 collection of interactive resources comprises a
3 collection of Web pages accessible through a Web site of
4 the enterprise.

1 45. Apparatus according to claim 43, wherein the server
2 is arranged to associate non-uniform privacy policies
3 with the resources, and to receive and store different
4 items of the information subject to different privacy
5 rules from among the non-uniform privacy policies.

1 46. Apparatus according to claim 45, wherein the server
2 is arranged to check the compliance of the application
3 with the privacy rules respectively applicable to each of
4 the items of the information requested by the
5 application.

1 47. Apparatus according to claim 45, wherein when the
2 server is arranged, upon determining that the application
3 does not comply with the rules respectively applicable to
4 a given one of the items, to refuse to provide the
5 requested information with respect to the given item,
6 while providing information regarding another of the
7 items with respect to which the application does comply
8 with the respectively applicable rules.

1 48. Apparatus according to claim 43, wherein the server
2 is arranged to receive the items from first and second
3 ones of the users subject to respective first and second
4 privacy policies, and to check the compliance of the
5 application with both the first and the second privacy
6 policies.

1 49. Apparatus according to claim 41, wherein the server
2 is adapted to make a record of the request and of the

3 information provided responsive thereto in a log for
4 review in a subsequent privacy audit.

1 50. A computer software product for privacy management,
2 comprising a computer-readable medium in which program
3 instructions are stored, which instructions, when read by
4 a computer, cause the computer to provide a linked
5 collection of interactive resources through which a user
6 is able to exchange information with an enterprise that
7 provides the resources, to assign respective, non-uniform
8 privacy policies to at least some of the resources
9 regarding use of the information that is exchanged
10 through the resources, to provide to a user who accesses
11 a given one of the resources the respective privacy
12 policy for that resource, and to exchange with the user
13 at least a portion of the information that is associated
14 with the given one of the resources, subject to the
15 provided privacy policy.

1 51. A product according to claim 50, wherein the
2 information exchanged with the user comprises private
3 information submitted to the enterprise by the user, and
4 wherein the instructions cause the computer to receive
5 and store the private information together with an
6 indication of the privacy policy agreed upon.

1 52. A product according to claim 50, wherein the
2 collection of resources comprises a collection of Web
3 pages accessible through a Web site of the enterprise.

1 53. A computer software product for privacy management,
2 comprising a computer-readable medium in which program
3 instructions are stored, which instructions, when read by
4 a computer, cause the computer to arrange a body of
5 information in a hierarchy of nodes that comprises a root

6 node, such that each of the nodes except for the root
7 node has a parent node in the hierarchy, to assign to
8 each of at least some of the nodes one or more respective
9 privacy rules regarding use of the information that is
10 associated with the node, to set for each of the nodes a
11 node privacy policy that comprises the privacy rules
12 assigned to the node combined, for each of the nodes
13 except the root node, with the node privacy policy of its
14 parent node, to provide to a user who accesses a given
15 one of the nodes the node privacy policy for that node,
16 and to exchange with the user at least a portion of the
17 information that is associated with the given one of the
18 nodes, subject to the provided privacy policy.

1 54. A computer software product for privacy management,
2 comprising a computer-readable medium in which program
3 instructions are stored, which instructions, when read by
4 a computer, cause the computer to provide a linked
5 collection of interactive resources through which a user
6 is able to exchange information with an enterprise that
7 provides the resources, at least some of the resources
8 having privacy policies associated therewith regarding
9 use of the information that is exchanged through the
10 resources, to receive information from users who access
11 the resources subject to the privacy policies, to
12 intercept a request from an application to use the
13 information received from the users, to query the
14 application to determine its compliance with the privacy
15 policies subject to which the requested information was
16 received, and to provide the requested information
17 subject to the compliance of the application with the
18 privacy policies.